SAP NetWeaver
IDENTITY MANAGEMENT

Berechtigungsworkflow
Keyuser's Guide

Andreas Schlüter

Version 2.1

Januar 2017

Inhalt

1. Allgemein

Die Verfahren zur Ausstattung der SAP-Anwender mit SAP-Berechtigungen werden durch standardisierte Verfahren mittels Web-Formulare des SAP NetWeaver Identity Managements(IdM) durchgeführt. Ziel ist es, die bisherigen Verfahren zu beschleunigen und flexibler, transparenter zu gestallten.

Der Berechtigungsworkflow wird auf folgende Objekte verwendet:

- Berechtigung
  - Eine Berechtigung entspricht einer SAP Rolle, einer SAP Sammelrolle, einem SAP Profil oder einer Java Gruppe in **einem** SAP System (und Mandant). Über Berechtigungen prüft das SAP System, ob z.B. ein Anwender eine Transaktion ausführen darf.
  - Z.B. „Z_BC_DRUCKEN“
  - Mitglieder einer Berechtigung im IdM haben automatisch die entsprechende Berechtigung im SAP System.
- Rolle (Geschäftsrolle)
  - Eine Rolle ist eine Sammlung von Berechtigungen einer oder **mehrerer** SAP Systeme.
  - Im IdM Kontext ist eine Rolle **keine** SAP Rolle, wie sie in den SAP Systemen Anwendung finden. *Geschäftsrolle* oder *IdM-Rolle* können synonym benutzt werden.
  - Mitglieder einer Rolle haben automatisch die in der Rolle enthaltenden Berechtigungen.
  - Eine Rolle wird i.d.R. im IdM als *Geschäftsrolle* modelliert, z.B. die Rolle „Sachbearbeiter“.

Am Berechtigungsworkflow sind vier Akteure beteiligt:

- Anwender
  - „Mir fehlen Berechtigungen!“
- Antragsteller
  - „Ich weiß, welche Berechtigungen meine Kollegen brauchen um Ihre Aufgaben erledigen zu können.“
  - i.d.R. dezentral
  - z.B. Keyuser
- Genehmiger
  - „Ich bin verantwortlich für IT-Verfahren und Anwendungen. Ich weiß, wer was machen darf.“

- i.d.R. zentral
- unterschreibt Benutzeranträge

- Berichtsempfänger
  - „Ich muss wissen, wer welche Berechtigungen zugewiesen bekommt."
  - z.B. Gesamtpersonalrat

1.1 Neuerungen der aktuellen Version

In der aktuellen Version SAP Identity Management 7.2 gibt es zur Vorgängerversion die folgenden wichtigen Änderungen:

- **Genehmigungsworkflow**:
  - Für den Genehmigungsworkflow gelten diese Regeln:
    - Antragsteller und Genehmiger müssen unterschiedliche Personen sein.
    - Anwender und Genehmiger müssen unterschiedliche Personen sein.
    - Anwender und Antragsteller können identisch sein.

      Beispiel 1:
      Person A beantragt für sich selbst eine Rolle. Person B genehmigt für Person A. Person A kann nicht genehmigen.

      Beispiel 2:
      Person C beantragt für Person A eine Rolle. Person B genehmigt für Person A. Person A und C können nicht genehmigen.

  - Genehmigungen können delegiert werden.
  - Abwesenheitsdelegationen z.B. bei Urlaub können eingerichtet werden.

- **SAP GUI Zugang und Account-Generierung**:
  - Die Rolle *Basis-Authentifizierung <Systemname>*
    - Existiert für jedes SAP System.
    - Nur Mitglieder dieser Rolle werden im jeweiligen SAP System tatsächlich angelegt.

- Nur Mitglieder dieser Rolle erhalten einen Passwort-Zugang für den SAP GUI.
- Nur für Mitglieder dieser Rolle können im *Elsa-Portal -> Identity Management* ein neues Initial-Passwort im entsprechendem SAP System vergeben werden.

- **Berechtigungen und Rollen beantragen**:
  - Der Task *Berechtigungen und Rollen beantragen*
    - Ersetzt den Task *Rolle beantragen.*
    - Ersetzt den Task *Berechtigung beantragen.*

1.2 Anmeldung am ELSA-Portal

Die Vergabe und Genehmigung von Berechtigungen erfolgt durch die Web-Anwendung des IdMs innerhalb des ELSA-Portals. Es wird empfohlen, zur Anmeldung ausschließlich den **Internet Explorer** zu verwenden. Die Anmeldung erfolgt mittels folgender URL:

- https://elsa.fu-berlin.de
- Geben Sie hier Ihren ZEDAT Benutzernamen und Passwort ein.
- Starten Sie die Portal-Anwendung „Identity Management“.

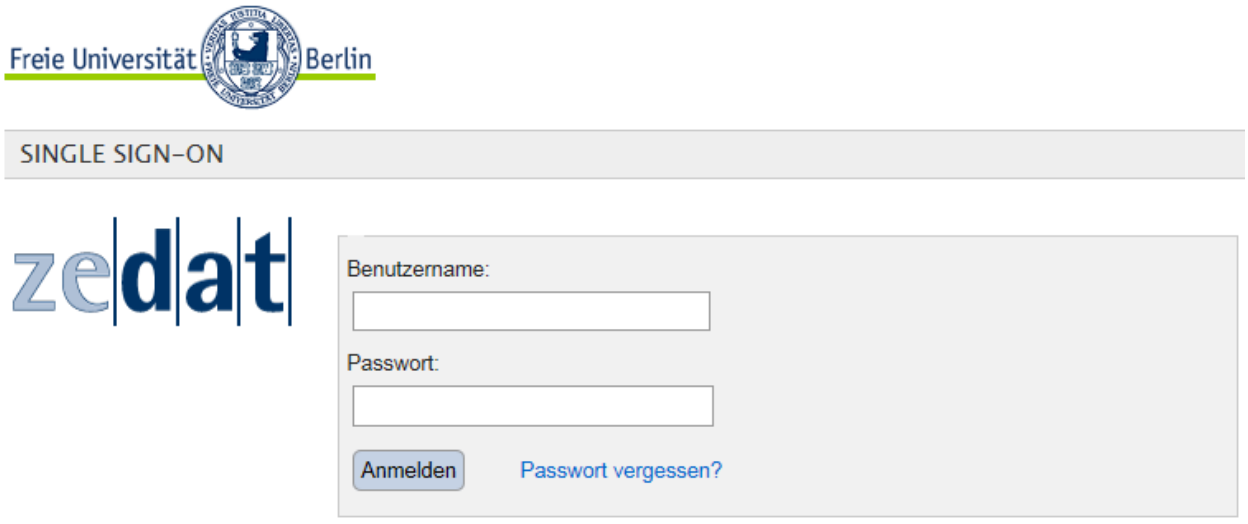

Abbildung 1 Anmeldung am ELSA-Portal

Abbildung 2 Portal-Anwendung „Identity Management“

2. Self-Services

Jeder Keyuser ohne weitere Berechtigungen, hat die Tabreiter „*Self-Services*“, „*Zu erledigen*“ und „*Verwalten*“ zur Verfügung. Im Self-Service-Tab lassen sich Änderungen am **eigenen** Benutzerkonto vornehmen: Sprache festlegen, Konto in einem SAP-System entsperren oder ein neues Passwort für das jeweilige System festlegen.

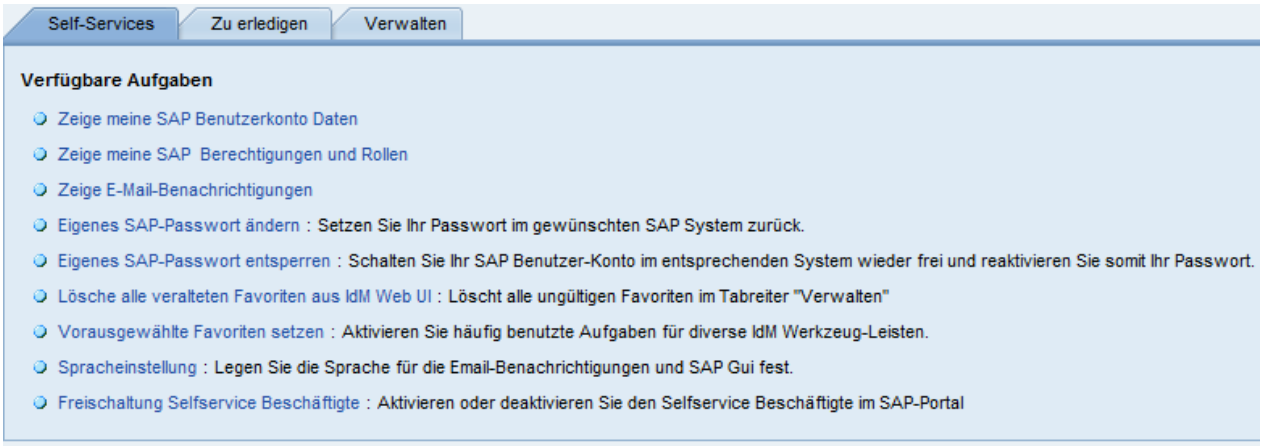

Abbildung 3 Startseite IdM Web-Anwendung

2.1.1 Eigenes SAP-Passwort zurücksetzen

Es folgt ein Beispiel, in dem gezeigt wird, wie sich der Benutzer *TESTKUH* für das System IT0 das Passwort zurücksetzen lässt.

Abbildung 4 Eigenes SAP-Passwort ändern

- Tabreiter *Self-Service* klicken.
- Aufgabe *Eigenes SAP-Passwort ändern* klicken (Abb. 3)
- Im neuen Browserfenster das entsprechende SAP-System wählen, hier IT0 wählen und ein Initialpasswort vergeben. (Abb. 4)
- Beim nächsten Einloggen in dieses System dieses Initialpasswort verwenden und anschließend ein neues vergeben.

Achtung: Es werden nur Systeme zur Wahl gestellt, in welchen Sie als User vorhanden sind und die Passwort-Anmeldung Ihnen gestattet ist. Systeme, in welchen Ihnen nur ein Web-Zugang erlaubt ist, tauchen nicht auf.

Hinweis: Fehlt ein System in der Auflistung, können Sie überprüfen, ob das Benutzerkonto die Rolle *Basis-Authentifizierung <Systemname>* hat (s.u.).

3. Personen verwalten

Um für Benutzer Berechtigungen und Rollen zu beantragen oder Anträge zu bearbeiten, verwenden Sie die Tabreiter:

- *Zu erledigen*
  - Hierüber können alle Anträge bearbeitet werden, für welche Sie als Genehmiger angegeben sind.
- *Verwalten*
  - Sie können in diesen Tabreiter unter anderem für Benutzer Berechtigungen oder Rollen beantragen.

3.1 Eine Person im IdM suchen und anzeigen

- Tabreiter Verwalten wählen
- *Anzeigen: Person* wählen, sofern dieses nicht schon ausgewählt ist.
- Im Feld *suchen* den Namen der Person, den ZEDAT-Account oder die Personalnummer hier eintragen (Abb.5.1)
  - Sie können auch Wildcards benutzen, z.B.:
  - „*Jung“ -> liefert alle Personen, deren Name mit „Jung“ endet
- *Start* klicken (Abb.5.2)

Abbildung 5 Suchen einer Person

- Für eine erweiterte Suche muss auf der rechten Seite des Formulars der Link *erweitert* aktiviert werden (Abb.5.3)
- Es kann so direkt über den Vornamen oder Nachnamen, etc. gesucht werden (Abb.6.1).

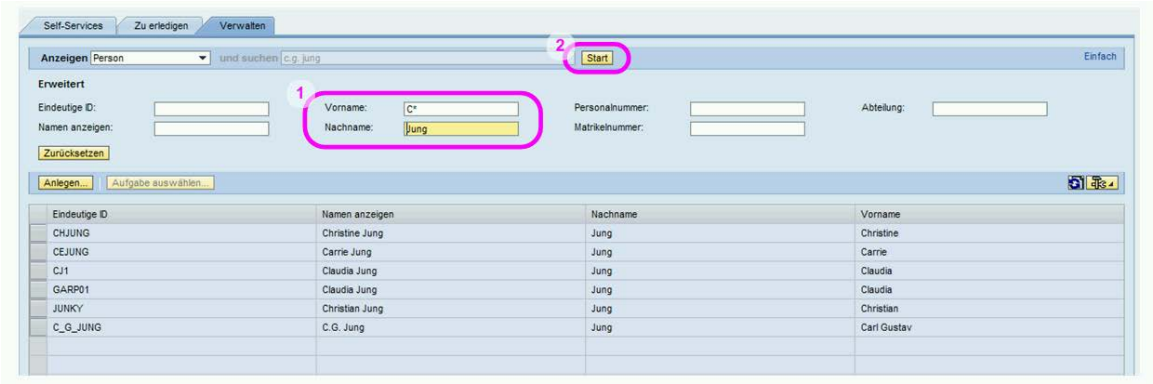

Abbildung 6 Erweiterte Suche nach einer Person

Es kann durchaus passieren, dass in der Ergebnisliste mehre Personeneinträge zu sehen sind. Um mittels der Detailübersicht die gewünschte Person zu finden, gehen Sie folgendermaßen vor:

- Die mögliche Person in der Ergebnisliste auswählen (Abb.7.1).
- Im unteren Bereich des Formulars sehen sie nun eine Detailübersicht
  - Tabreiter *Allgemein* (Abb.7.2) gibt eine kurze Übersicht
  - Tabreiter *Rollen und Berechtigungen* (Abb.7.3) zeigt alle Berechtigungen und Rollen, die der Person erteilt wurden.

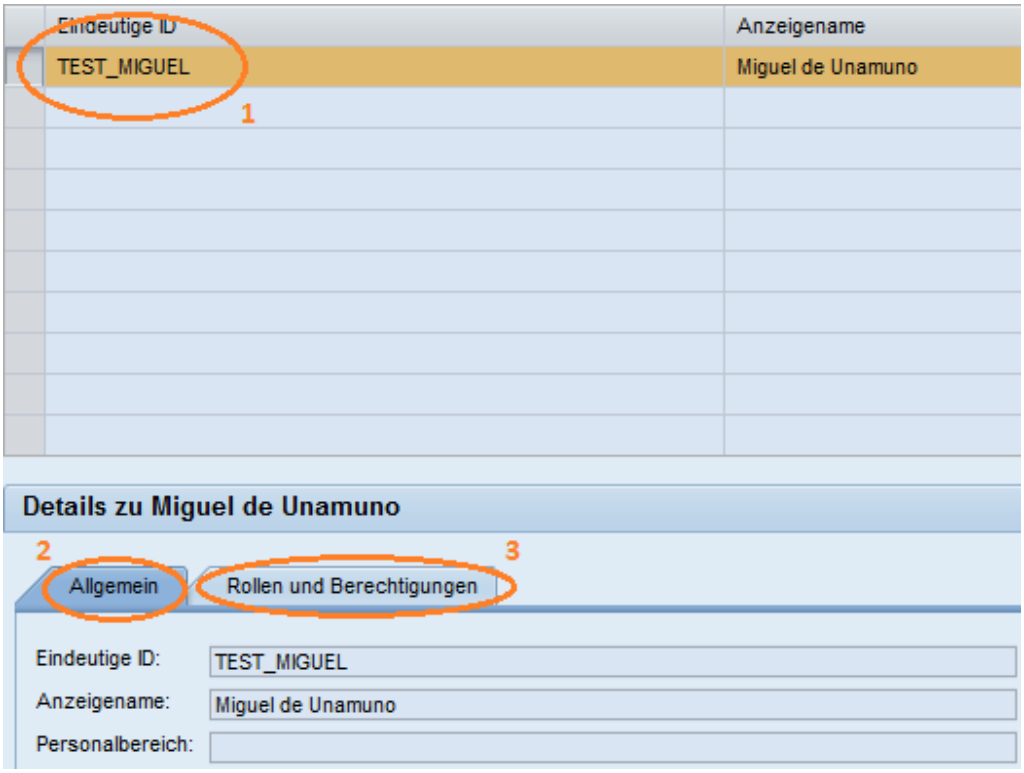

Abbildung 7 Detailübersicht zu einer Person

Um sich eine Person komplett anzeigen zu lassen, sind folgende Schritte nötig:

- Die gewünschte Person in der Ergebnisliste auswählen (Abb.8.1).
- Knopf *Aufgabe auswählen* klicken(Abb.8.2)
- Im Popup-Fenster den *Person*-Knoten öffnen, dazu auf den kleinen Pfeil links neben *Person* klicken (Abb.8.3).
- Aufgabe *Person anzeigen* auswählen (Abb.8.4).
- *Aufgabe auswählen* klicken (Abb.8.5).
  - **Hinweis**: Sie können Sich hier auch Ihre oft genutzten Aufgaben als Favoriten zu Ihren *Verwalten*-Formular hinzufügen, dazu wählen sie statt *Aufgabe auswählen* den Knopf *Zu Favoriten hinzufügen* aus

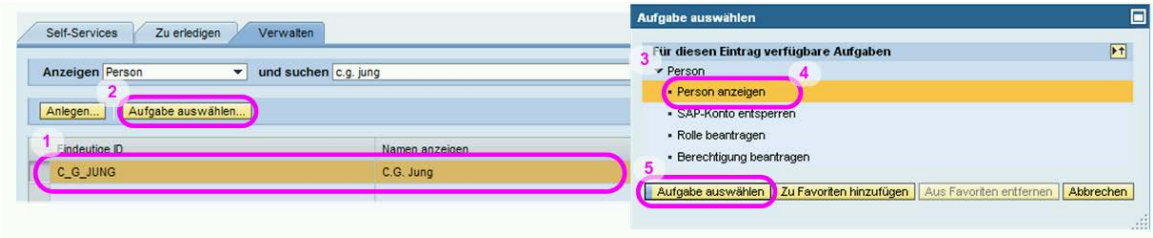

Abbildung 8 Aufgabe *Person anzeigen* aufrufen

3.2 Rolle/Berechtigung für einen Anwender beantragen

Müssen eine oder mehrere Rollen/Berechtigungen einer Person zugeordnet werden, folgen Sie den Schritten.

- Person suchen
  - Tabreiter Verwalten wählen
  - *Anzeigen: Person* wählen, sofern dieses nicht schon ausgewählt ist.
  - Im Feld *suchen* den Namen der Person, das ZEDAT Account oder die Personalnummer hier eintragen (Abb.5.1)
    - Sie können auch Wildcards benutzen, z.B:
    - „*Jung“ -> liefert alle Personen, deren Name mit „Jung“ endet
  - *Start* klicken (Abb.5.2)

- Aufgabe *Berechtigungen und Rollen beantragen* aufrufen
  - Die gewünschte Person in der Ergebnisliste auswählen (Abb.9.1).
  - Knopf *Aufgabe auswählen* klicken(Abb.9.2)
  - Im Popup-Fenster den *Person*-Knoten öffnen, dazu auf den kleinen Pfeil links neben *Person* klicken (Abb.9.3).
  - *Berechtigungen und Rollen beantragen* auswählen (Abb.9.4).
  - *Aufgabe auswählen* klicken (Abb.9.5).
    - **Hinweis**: Sie können Sich hier auch Ihre oft genutzten Aufgaben als Favoriten zu Ihren *Verwalten*-Formular hinzufügen, dazu wählen sie statt *Aufgabe auswählen* den Knopf *Zu Favoriten hinzufügen* aus

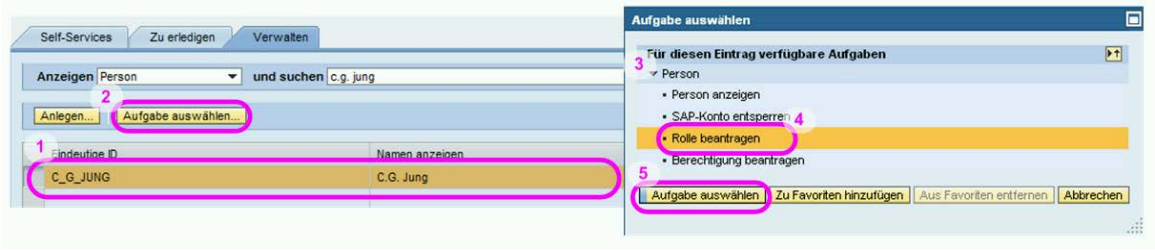

Abbildung 9 Aufgabe *Rolle beantragen* aufrufen

- Rollen/Berechtigungen hinzufügen
  - Im linken *Dropdown-Menü* Rolle oder Berechtigung wählen (Abb.10.1.1)
  - Im *Suchen*-Feld gewünschte Rolle/Berechtigung eingeben und auf *Suchen* klicken (Abb.10.1.2)
  - Gewünschte Rolle/Berechtigung aus der linken Ergebnisliste wählen (Abb.10.1.3)
  - Knopf *Hinzufügen* klicken (Abb.10.1.4)

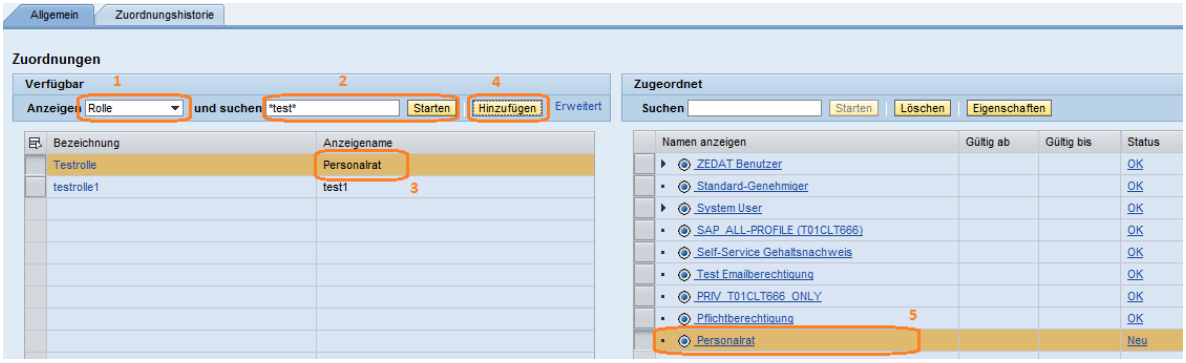

Abbildung 5.1 *Rolle/Berechtigung* suchen

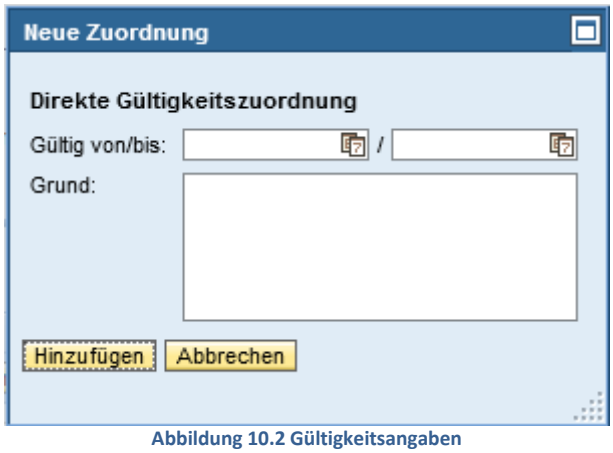

Abbildung 10.2 Gültigkeitsangaben

- Rolle zeitlich begrenzen, wenn nötig (Abb.10.2)
  - *Gültig ab, Gültig bis* beschränken die Zuordnung zeitlich. Dem Anwender werden automatisch zum Zeitpunkt *Gültig ab* die Rolle zugewiesen, sowie zum Zeitpunkt *Gültig bis* automatisch diese wieder entfernt.
  - *Grund* des Antrages ist für den Genehmiger sichtbar. Beispiel: „Urlaubsvertretung für Fr. Anima“

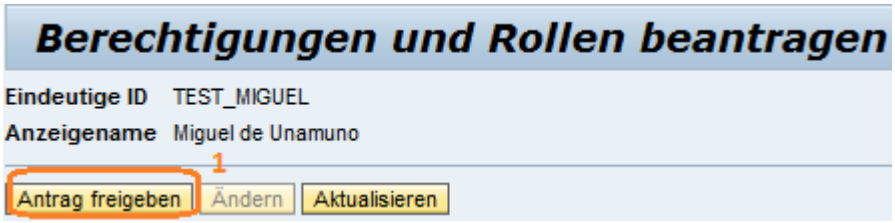

Abbildung 10.3 Antrag freigeben

- Antrag freigeben (Abb.10.3.1).

Ergebnis:

Sämtliche Genehmiger dieser Rolle(n)/Berechtigung(en) werden per E-Mail über den Antrag informiert. Nach Genehmigung wird die Rolle/ Berechtigung dem Anwender zugeordnet und in den einzelnen SAP-Systemen zugewiesen. Sofern der Anwender im SAP-System neu angelegt wird, muss sich dieser im Elsa-Portal per IdM Self Service ein Initialpasswort kreieren.

ACHTUNG:

Falls Sie für einen User eine **Berechtigung** beantragt haben, **muss**

1. entweder für einen SAP GUI Zugang:
   diesem User zusätzlich die Rolle ***BASIS-AUTHENTIFIZIERUNG*** für dasselbe SAP-System beantragt werden,

2. oder für einen Web-Zugang:
   diesem User zusätzlich die Berechtigung ***PRIV_< SAP-System>_ONLY*** für dasselbe SAP-System beantragt werden,

falls er diese noch nicht hat.

Dadurch wird der Benutzer im SAP-System angelegt und ggf. einen Passwort-Zugang ermöglicht. Ohne diese Rolle werden keine andere Rollen/Berechtigungen im SAP System zugewiesen.

3.3 Details zu Berechtigungen und Rollen eines Users

Die Darstellung von Berechtigungen und Rollen zu einem User im IdM bietet einige hilfreiche Features:

- Unter den linken Button „Mehr Filter“ findet man Möglichkeiten Versteckte Zuordnungen anzeigen zu lassen:
  - Künftig: es werden Zuordnungen angezeigt, welche erst in Zukunft gültig sind.
  - Historie: es werden Zuordnungen angezeigt, die der User verloren hat.
  - Nur direkt: alle vererbten Zuordnungen werden ausgeblendet.
- Zuordnungen können einen Status aus folgender Liste haben:
  - Ok: Berechtigungen wurden ins SAP System übernommen
  - In Bearbeitung: entweder muss die Zuordnung noch genehmigt werden oder es wird gerade ins SAP System geschrieben.
  - Fehlgeschlagen (nur sichtbar im Task Berechtigung und Rollen beantragen): es ist ein Fehler aufgetreten. Tipp: Sie können auf den Status klicken und die Zuordnung wiederholen lassen.
  - Abgelehnt: Zuordnung wurde vom Genehmiger abgelehnt.
- Der Button Eigenschaften oder ein Klick auf den Status einer Zuordnung öffnet ein Fenster, indem Sie z.B. in Erfahrung bringen können, wer die Zuordnung beantragt oder genehmigt hat.

3.4 Mitglieder für eine Rolle beantragen

So wie Sie für eine Person eine Rolle beantragen, können Sie auch zu einer Rolle Mitglieder beantragen. Das Ergebnis ist das Gleiche. Der Vorteil letzterer Methode ist, dass Sie so mit einer Aktion gleich eine Menge von Personen einer Rolle zuordnen können. Im folgenden Beispiel wird der Rolle *IdM Experte* die komplette Abteilung *eAS* hinzugefügt. Mitgliedschaften für Berechtigungen funktionieren analog.

- Rollen suchen
  - Tabreiter Verwalten wählen
  - *Anzeigen:* ***Rolle*** (Abb.11.1)

- **Hinweis**: Für Berechtigungen ist *Anzeigen: Berechtigung* zu wählen.

- Im Feld *suchen* gewünschte Rolle eintragen und auf *Start* klicken (Abb.11.2)

- Aufgabe *Mitgliedschaft beantragen* aufrufen

  - Gewünschte Rolle aus der Ergebnisliste wählen (Abb.10.3)

  - Knopf *Aufgabe auswählen* klicken (Abb.10.3)

  - Im Popup-Fenster den *Rolle*-Knoten öffnen, dazu auf den kleinen Pfeil links neben *Rolle* klicken (Abb.9.3).

  - Aufgabe *Mitgliedschaft beantragen* auswählen (Abb.8.4).

    - **Hinweis**: Für Berechtigungen ist die gleiche Aufgabe zu wählen.

  - *Aufgabe auswählen* klicken.

    - **Hinweis**: Sie können Sich hier auch Ihre oft genutzten Aufgaben als Favoriten zu Ihren *Verwalten*-Formular hinzufügen, dazu wählen sie statt *Aufgabe auswählen* den Knopf *Zu Favoriten hinzufügen* aus

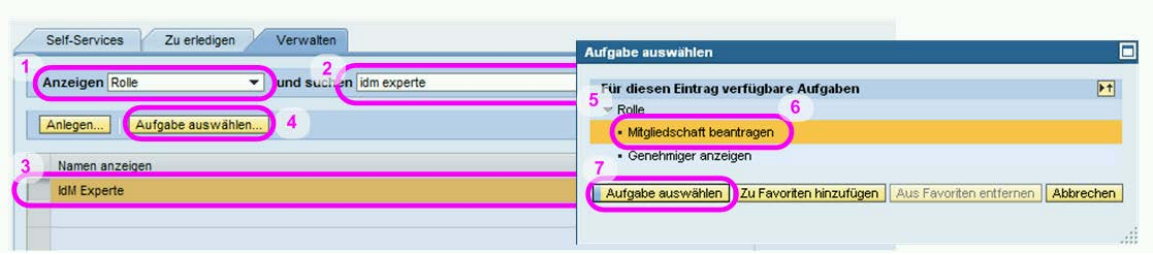

Abbildung 6 *Aufgabe Mitgliedschaft für Rolle beantragen* starten

- Mitglieder hinzufügen

  - Erweiterte suche aktivieren durch klicken auf *erweitert* (Abb.12.1)

  - Die Person oder den Personenkreis bestimmen und auf *suchen* klicken. Z.B. Abteilung = „Electronic Administration and Services“ ergibt alle Personen der Abt. eAS.

  - Gewünschte Personen auswählen (+STRG oder +SHIFT Taste bei Mehrfachauswahl). Sie können auch die komplette Liste auswählen durch klicken auf das Tabelleauswahlmenu (Abb.12.3) und dann auf *Alles auswählen* (Abb.12.4).

  - *Hinzufügen* klicken (Abb.12.6)

  - Sichern (Abb.12.6)

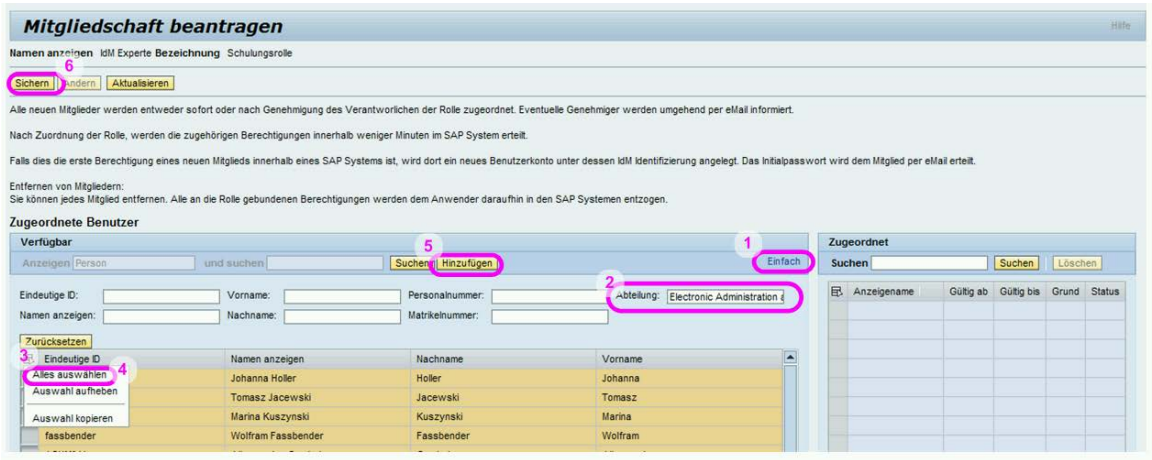

Abbildung 7 Mehrere Personen zu Rolle hinzufügen

Ergebnis:

Sie haben eine oder mehrere Personen einer Rolle zugewiesen. Jede einzelne Person muss genehmigt werden. Alle beteiligten Genehmiger werden per Email informiert und die Anwender per Email über die Entscheidung der Genehmiger.

3.5 Antrag genehmigen

I.d.R. werden Sie per Email informiert, wenn von Ihnen eine Entscheidung über einen Rollen- oder Berechtigungsantrag vom IdM erwartet wird. Im Tabreiter *Zu erledigen* sind alle Anträge aufgelistet, welche von **Ihnen** bearbeitet werden müssen.

- Antrag auswählen
  - Tabreiter *Zu erledigen*
  - In der Liste der Anträge wählen sie einen Antrag aus (Abb.13.1).
  - Zu dem ausgewählten Antrag erhalten sie eine Detailübersicht im unteren Teil des Formulars:
    - Welche Rolle oder Berechtigung wurde beantragt (Abb.13.2)?
    - Wer hat den Antrag gestellt (Abb.13.3)?
    - Wer kann diesen Antrag noch genehmigen (Abb.13.4)?

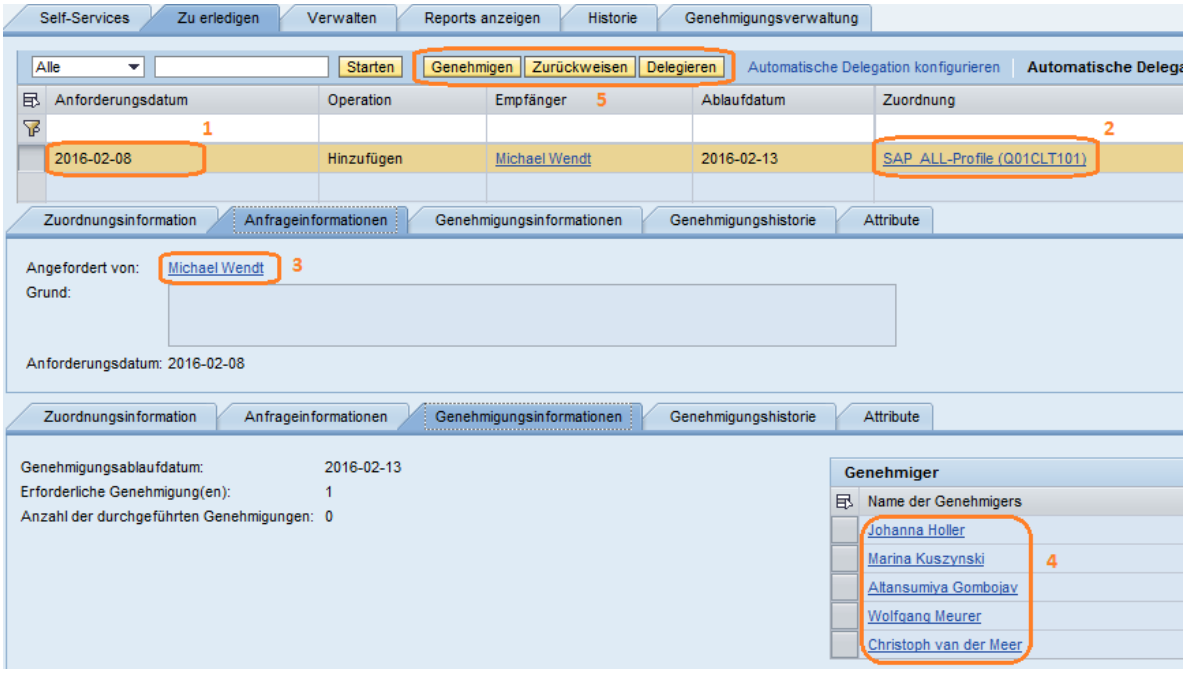

Abbildung 8 Tabreiter *Zu erledigen*

- Antrag bearbeiten (Abb.13.5)

- *Genehmigen*: Antrag wird genehmigt und Rolle/Berechtigung zugeordnet.
- *Zurückweisen*: Antrag wird abgelehnt → keine Zuordnung.
- *Delegieren*: Für den Fall, dass Sie die Entscheidung nicht treffen wollen, können Sie diese weiterleiten. Eine andere Person, die Zugang zum „*zu erledigen*“ Tabreiter hat, erhält dann diese Anfrage.

Ergebnis:

Der Anwender wird über Ihre Entscheidung informiert.

Falls der Anwender im entsprechenden SAP-System noch kein Benutzerkonto besitzt, so wird dieses angelegt, sofern der Anwender die Rolle **Basis-Authentifizierung** für dieses System ebenfalls besitzt. Der Anwender erhält dann ggf. eine E-Mail (in Produktivsystem definitiv, in Test- und Quali-Systemen nicht), in der er aufgefordert wird, sich über das ELSA-Portal ein **neues Passwort** für dieses SAP-System zu vergeben.

ACHTUNG:

- Für den Genehmigungsworkflow gelten diese Regeln:
  - Antragsteller und Genehmiger müssen unterschiedliche Personen sein.
  - Anwender und Genehmiger müssen unterschiedliche Personen sein.
  - Anwender und Antragsteller können identisch sein.

Sowohl Antragsteller als auch Anwender werden auch im Falle, dass sie selbst als Genehmiger angegeben sind, diese Genehmigung im Tabreiter „zu erledigen“ nicht zu sehen bekommen.